Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (cancelled)

2. (cancelled)

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (previously presented) A process of detecting security vulnerabilities present in a target Web site, comprising:

establishing an Internet connection with the target Web site;

retrieving a default Web page for the target Web site;

parsing through the default Web page to identify any linked-to Web pages or objects which are included in the default Web page;

automatically passing an authorized username and password to the target Web site, if required to gain access to the target Web site;

scanning the target Web site for at least one known exploit in order to identify security vulnerabilities;

applying at least one predetermined hack method to the target Web site in order to identify security vulnerabilities; and

outputting the security vulnerabilities.

BEST AVAILABLE COPY

PAGE 4/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

7. (previously presented) The method of claim 6, further comprising scanning at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities.

8. (previously presented) The method of claim 6, further comprising parsing through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages.

9. (previously presented) The method of claim 8, further comprising parsing through the default Web page to identify any hidden Web pages or objects which are included in the hidden Web pages.

10. (previously presented) The method of claim 9, further comprising parsing through the hidden Web-pages to identify any further-hidden Web pages or objects which are included in the further-hidden Web pages.

11. (previously presented) The method of claim 10, further comprising:

comparing each hidden Web page and each further-hidden Web page to each linked-to Web page and each further-linked-to Web page; and

identifying each hidden Web page and each further-hidden Web page that is different from the linked-to Web pages and the further-linked to Web pages.

12. (previously presented) The method of claim 8, wherein the parsing through the default Web page and the parsing through the linked-to Web pages include performing a keyword search in order to detect at least one point of interest.

PAGE 5/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

13. (previously presented) The method of claim 12, wherein the at least one point of interest is selected from the group consisting of an administration Web page and a directory list tag.

14. (previously presented) The method of claim 12, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory.

15. (previously presented) The method of claim 8, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory.

16. (previously presented) The method of claim 15, wherein the scanning the target Web site for at least one known exploit includes checking for at least one common filename.

17. (previously presented) The method of claim 16, wherein the at least one common filename is selected from the group consisting of "msadcs.dll" and "WS_FTP.LOG."

18. (previously presented) The method of claim 8, wherein the applying at least one predetermined hack method includes automatically passing multiple usernames and passwords to the target Web site if a login Web page is encountered.

19. (previously presented) A process of detecting security vulnerabilities present in a target Web site, comprising:

establishing an Internet connection with the target Web site;

retrieving a default Web page for the target Web site;

PAGE 6/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

parsing through the default Web page to identify any linked-to Web pages or objects which are included in the default Web page, wherein the parsing includes performing a keyword search in order to detect at least one point of interest;

scanning the target Web site for at least one known exploit in order to identify security vulnerabilities;

applying at least one predetermined hack method to the target Web site in order to identify security vulnerabilities; and

prioritizing the security vulnerabilities.

20. (previously presented) The method of claim 19, further comprising parsing through the default Web page to identify any hidden Web pages or objects which are included in the hidden Web pages.

21. (previously presented) The method of claim 20, further comprising parsing through the hidden Web-pages to identify any further-hidden Web pages or objects which are included in the further-hidden Web pages.

22. (previously presented) The method of claim 21, further comprising:

comparing each hidden Web page and each further-hidden Web page to each linked-to Web page and each further-linked-to Web page; and

identifying each hidden Web page and each further-hidden Web page that is different from the linked-to Web pages and the further-linked to Web pages.

23. (previously presented) The method of claim 19, further comprising parsing through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages.

PAGE 7/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

24. (previously presented) The method of claim 23, wherein the at least one point of interest is selected from the group consisting of an administration Web page and a directory list tag.

25. (previously presented) The method of claim 23, further comprising scanning at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities.

26. (previously presented) The method of claim 23, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory.

27. (previously presented) The method of claim 23, further comprising automatically passing an authorized username and password to the target Web site, if required to gain access to the target Web site.

28. (previously presented) The method of claim 23, wherein the applying at least one predetermined hack method includes automatically passing multiple usernames and passwords to the target Web site if a login Web page is encountered.

29. (previously presented) The method of claim 23, wherein the applying at least one predetermined hack method includes passing invalid data to a data entry field of the target Web site and evaluating the result.

30. (previously presented) The method of claim 29, further comprising:

recording the invalid data which produces a security vulnerability; and

passing the recorded invalid data to at least one other data entry field of the target Web site.

PAGE 8/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

31. (previously presented) A process of detecting security vulnerabilities present in a target Web site, comprising:

establishing an Internet connection with the target Web site;

retrieving a default Web page for the target Web site;

parsing through the default Web page to identify any linked-to Web pages or objects which are included in the default Web page;

scanning the target Web site for at least one known exploit in order to identify security vulnerabilities;

applying at least one predetermined hack method to the target Web site in order to identify security vulnerabilities, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory; and

outputting the security vulnerabilities.

32. (previously presented) The method of claim 31, further comprising scanning at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities.

33. (previously presented) The method of claim 31, further comprising parsing through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages.

34. (previously presented) The method of claim 33, further comprising parsing through the default Web page to identify any hidden Web pages or objects which are included in the hidden Web pages.

PAGE 9/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

35. (previously presented) The method of claim 34, further comprising parsing through the hidden Web-pages to identify any further-hidden Web pages or objects which are included in the further-hidden Web pages.

36. (previously presented) The method of claim 35, further comprising:

comparing each hidden Web page and each further-hidden Web page to each linked-to Web page and each further-linked-to Web page; and

identifying each hidden Web page and each further-hidden Web page that is different from the linked-to Web pages and the further-linked to Web pages.

37. (previously presented) The method of claim 33, wherein the parsing through the default Web page and the parsing through the linked-to Web pages include performing a keyword search in order to detect at least one point of interest.

38. (previously presented) The method of claim 37, wherein the at least one point of interest is selected from the group consisting of an administration Web page and a directory list tag.

39. (previously presented) The method of claim 38, further comprising automatically passing an authorized username and password to the target Web site, if required to gain access to the target Web site.

40. (previously presented) The method of claim 33, wherein the scanning the target Web site for at least one known exploit includes checking for at least one common filename.

PAGE 10/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

41. (previously presented) The method of claim 40, wherein the at least one common filename is selected from the group consisting of "msadcs.dll" and "WS_FTP.LOG."

42. (previously presented) A system for detecting security vulnerabilities present in a target Web site, comprising:

memory for storing:

a Web page database;

at least one exploit; and

a security vulnerability database; and

a processor connected to the memory and being configured to:

establish an Internet connection with the target Web site;

retrieve a default Web page for the target Web site;

parse through the default Web page to identify any linked-to Web pages or objects which are included in the default Web page;

automatically pass an authorized username and password to the target Web site, if required to gain access to the target Web site;

scan the target Web site for at least one known exploit in order to identify security vulnerabilities;

apply at least one predetermined hack method to the target Web site in order to identify security vulnerabilities; and

prioritize the security vulnerabilities.

PAGE 11/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

43. (previously presented) The system of claim 42, wherein the processor is further configured to parse through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages.

44. (previously presented) The system of claim 43, wherein the processor is further configured to scan at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities.

45. (previously presented) The system of claim 44, wherein the processor is further configured to parse through the default Web page to identify any hidden Web pages or objects which are included in the hidden Web pages.

46. (previously presented) The system of claim 45, wherein the processor is further configured to parse through the hidden Web-pages to identify any further-hidden Web pages or objects which are included in the further-hidden Web pages.

47. (previously presented) The system of claim 46, wherein the processor is further configured to:

compare each hidden Web page and each further-hidden Web page to each linked-to Web page and each further-linked-to Web page; and

identify each hidden Web page and each further-hidden Web page that is different from the linked-to Web pages and the further-linked to Web pages.

48. (previously presented) The system of claim 43, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory.

PAGE 12/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

49. (previously presented) The system of claim 48, wherein the parsing through the default Web page and the parsing through the linked-to Web pages include performing a keyword search in order to detect at least one point of interest.

50. (previously presented) The system of claim 49, wherein the at least one point of interest is selected from the group consisting of an administration Web page and a directory list tag.

51. (previously presented) The system of claim 43, wherein the applying at least one predetermined hack method includes automatically passing multiple usernames and passwords to the target Web site if a login Web page is encountered.

52. (previously presented) A system for detecting security vulnerabilities present in a target Web site, comprising:

memory for storing:

a Web page database;

at least one exploit; and

a security vulnerability database; and

a processor connected to the memory and being configured to:

establish an Internet connection with the target Web site;

retrieve a default Web page for the target Web site;

parse through the default Web page to identify any linked-to Web pages or objects which are included in the default Web page, wherein the parsing includes performing a keyword search in order to detect at least one point of interest;

PAGE 13/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

scan the target Web site for at least one known exploit in order to identify security vulnerabilities;

apply at least one predetermined hack method to the target Web site in order to identify security vulnerabilities; and

output the security vulnerabilities.

53. (previously presented) The system of claim 52, wherein the processor is further configured to scan at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities.

54. (previously presented) The system of claim 52, wherein the processor is further configured to parse through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages.

55. (previously presented) The system of claim 54, wherein the at least one point of interest is selected from the group consisting of an administration Web page and a directory list tag.

56. (previously presented) The system of claim 54, wherein the processor is further configured to parse through the default Web page to identify any hidden Web pages or objects which are included in the hidden Web pages.

57. (previously presented) The system of claim 56, wherein the processor is further configured to parse through the hidden Web-pages to identify any further-hidden Web pages or objects which are included in the further-hidden Web pages.

58. (previously presented) The system of claim 57, wherein the processor is further configured to:

PAGE 14/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

compare each hidden Web page and each further-hidden Web page to each linked-to Web page and each further-linked-to Web page; and

identify each hidden Web page and each further-hidden Web page that is different from the linked-to Web pages and the further-linked to Web pages.

59. (previously presented) The system of claim 54, wherein the processor is further configured to automatically pass an authorized username and password to the target Web site, if required to gain access to the target Web site.

60. (previously presented) The system of claim 59, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory.

61. (previously presented) The system of claim 54, wherein the applying at least one predetermined hack method includes passing invalid data to a data entry field of the target Web site and evaluating the result.

62. (previously presented) The system of claim 61, wherein the processor is further configured to:

record the invalid data which produces a security vulnerability; and

pass the recorded invalid data to at least one other data entry field of the target Web site.

63. (previously presented) A system for detecting security vulnerabilities present in a target Web site, comprising:

memory for storing:

a Web page database;

PAGE 15/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

at least one exploit; and

a security vulnerability database; and

a processor connected to the memory and being configured to:

establish an Internet connection with the target Web site;

retrieve a default Web page for the target Web site;

parse through the default Web page to identify any linked-to Web pages or objects which are included in the default Web page;

scan the target Web site for at least one known exploit in order to identify security vulnerabilities;

apply at least one predetermined hack method to the target Web site in order to identify security vulnerabilities, wherein the applying at least one predetermined hack method includes attempting to access unauthorized files located outside the target Web site's root directory; and

output the security vulnerabilities.

64. (previously presented) The system of claim 63, wherein the processor is further configured to parse through the linked-to Web pages to identify any further-linked-to Web pages or objects which are included in the linked-to Web pages.

65. (previously presented) The system of claim 64, wherein the processor is further configured to parse through the default Web page to identify any hidden Web pages or objects which are included in the hidden Web pages.

PAGE 16/19 * RCVD AT 10/8/2004 4:32:02 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:404 815 3509 * DURATION (mm-ss):04-48

66. (previously presented) The system of claim 65, wherein the processor is further configured to parse through the hidden Web-pages to identify any further-hidden Web pages or objects which are included in the further-hidden Web pages.

67. (previously presented) The system of claim 66, wherein the processor is further configured to:

compare each hidden Web page and each further-hidden Web page to each linked-to Web page and each further-linked-to Web page; and

identify each hidden Web page and each further-hidden Web page that is different from the linked-to Web pages and the further-linked to Web pages.

68. (previously presented) The system of claim 67, wherein the parsing through the default Web page and the parsing through the linked-to Web pages include performing a keyword search in order to detect at least one point of interest.

69. (previously presented) The system of claim 68, wherein the at least one point of interest is selected from the group consisting of an administration Web page and a directory list tag.

70. (previously presented) The system of claim 64, wherein the processor is further configured to automatically pass an authorized username and password to the target Web site, if required to gain access to the target Web site.

71. (previously presented) The system of claim 70, wherein the processor is further configured to scan at least one of the security vulnerabilities for at least one known exploit in order to identify further security vulnerabilities.

72. – 102. (cancelled)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.